PATENT
Attorney Docket No. 1948/US/2
USPTO Facsimile No. (703) 872-9306

Amendments to the Specification:

Please replace the paragraph beginning at page 17, line 6, (paragraph [00050]) with the following paragraph, marked to show changes:

[00050] It is to be appreciated that in mail-exchange server topologies, a recipient's system 125 or device (such as a personal computer) may include e-mail/communication software 130 that is configured to perform ranking and presentation, as appropriate, of franked communications 105. Similarly, in embodiments wherein a mail-exchange server ~~135~~ is not utilized or communications are not received via a local software application 130 and instead are received via a network or server based application (for example, from a communications feature provided by an ISP server or a remote computing application, such as that supported by Citrix Systems and other like systems), the filtering and ranking may occur at the service provider's (and/or a third party's) server or system instead of the recipient's system 125. The results of such filtering and ranking may be provided via HTML pages, XML pages, Flash implementations, Java implementations and/or any other types of information transfer formats supported by a given service provider and compatible with a recipient's given device(s). Commonly, but not necessarily, such information transfer may occur via Web browser compatible information formats, such as those supported by Microsoft Internet Explorer, Netscape Navigator and others.

Please replace the paragraph beginning at page 20, line 9, (paragraph [00058]) with the following paragraph, marked to show changes:

[00058] In another embodiment, the franking server, ~~mail server~~ network node 135 or other communications system, server, or switch may be configured to delay transmission of lower category e-mails/communications 105 until the recipient's e-mail/communication application program 130 indicates to the server that all franked e-mails/communications of a given or higher category have been received and presented to the recipient. It can be appreciated by those skilled in the art that the ability to filter, categorize, purge, prioritize, and/or delay certain communications, while expediting or processing others at a normal rate, may increase the efficiency of networked communication systems, such as the Internet, the World Wide Web, and others.

Please replace the paragraph beginning at page 20, line 21, (paragraph [00060]) with the following paragraph, marked to show changes:

[00060] One approach commonly advocated and sometimes implemented to control spam and/or other undesirable communications is to utilize filtering technologies.

One embodiment 200 of a filtering approach is shown in Fig. 2A. In the filtering approach, which is commonly implemented by ISPs and/or corporate e-mail/communication systems, a "filter" 205 screens and eliminates unwanted e-mails/communications 105 received via a communications network 120 (such as the Internet or other networks). Such e-mails/communications 105 may originate from a sender's ISP 215, associated sender system 115, and/or communications devices, may be "spoofed" as if sent from another person or e-mail/communication address, or may arrive at the filter 205 via various other paths. Regardless of the source or path, e-mails/communications 105 that "pass" through the filter 205 are delivered to the recipient's system 125, while e-mails/communications that do not pass through the filter are generally discarded into an e-mail/communication "dump" 220. It should be noted that, although Fig. 2A displays a single dump, in actuality each ISP, network node 135, and/or recipient's device(s) may maintain one or more dumps for filtered e-mails/communications 105. Accordingly, the single dump 220 illustrated in Fig. 2A is simplified.

Please replace the paragraph beginning at page 21, line 22, (paragraph [00062]) with the following paragraph, marked to show changes:

[00062] In order to filter unwanted e-mails/communications 105 from legitimate communications, ~~filter systems~~ filters 205 commonly attempt to determine whether the domain from which a given e-mail/communication has been sent is on a "banned" list (i.e., a list of domains associated with persons or entities from whom a recipient, ISP or others do not desire to receive communications, for example, a listing of known spammers). If so, the filter 205 generally automatically rejects e-mails/communications 105 from such domain(s). However, spammers constantly change, "spoof," and/or hijack legitimate domains and/or senders' systems 115, addresses and devices, and/or mask the domain from which they send spam. Thus, a cat and mouse game often ensues between spammers and anti-spammers (i.e., those wishing to eliminate spam), in which the anti-spammers attempt to rely upon and/or utilize filtering techniques to eliminate spam.

Please replace the paragraph beginning at page 22, line 11, (paragraph [00063]) with the following paragraph, marked to show changes:

[00063] Further, a major shortcoming of filters 205 and filtering systems is that they often have unintended consequences. As a filter becomes more specific in the content it does or does not allow to pass through, the filter may often reject undesired communications ~~105~~, such as spam, as well as legitimate communications. Additionally, filters 205 often do not reduce the volume of communications 105 received by any given ISP

225. Instead, filters 205 commonly reduce the volume of communications ~~105communicated~~ 105 communicated to a next node on a network and ultimately presented to a given recipient system 125.

Please replace the paragraph beginning at page 22, line 19, (paragraph [00064]) with the following paragraph, marked to show changes:

[00064] One embodiment of the present invention uses aspects of the above described filtering processes in conjunction with frank 110 processing rules and systems to determine which communications 105 to present to a recipient. Using this embodiment, ISPs 225 or other network nodes 135 or entities (including recipients) do not need to (but, may still do so if desired) utilize filters 205 to analyze an e-mail/communication ~~105and~~ 105 and determine whether the sender, recipient, address, subject or content of the e-mail/communication is of such nature that it is acceptable to present to a given recipient or network node. Instead, the ISP 225 or other network node 135 processes e-mails/communications 105 in accordance with pre-defined or real-time defined franking rules and/or preferences. As is discussed in greater detail below, franks 110 may be attached or otherwise associated with given e-mails/communications 105. For example, in the case of streaming media, a frank 110 might exist for a given time period for a given stream of information from a specified source(s).

Please replace the paragraph beginning at page 23, line 10, (paragraph [00065]) with the following paragraph, marked to show changes:

[00065] Rules may specify, for example, that only e-mails/communications 105 meeting specific franking requirements are presented to the recipient. Continuing the example, one such rule may provide that all unfranked e-mails/communications 105 are automatically discarded or rejected. Further, when a communication 105 is rejected, rules may provide for the transmission of a return e-mail/communication 105 indicating the reason for such rejection. Exemplary reasons include a lack of a frank 110, insufficient frank or the like. Similarly, rules may be developed such that e-mails/communications 105 that are not franked with a specific class of frank ~~105~~ 110, or are not transmitted from a sender on an approved sender list (even if franked) are processed in accordance with other rules or procedures. Further, rules may provide that e-mails/communications 105 associated with a streaming media frank are processed first, in order to prevent jitter or other undesired interruptions in any e-mails/communications. It should also be appreciated that any rules and associated processing of e-mails/communications 105 may be handled by any ISP 225, server, intermediate network node 135, router, and so forth (collectively, "network node" 135)

along the transmission path of the e-mail/communication ~~435~~ 105, including the sender's ~~own~~ ISP 215.

Please replace the paragraph beginning at page 24, line 4, (paragraph [00066]) with the following paragraph, marked to show changes:

[00066] By separating the filtering of content (which may still occur in conjunction with the present invention) from the processing of franked/unfranked e-mails/communications 105 (which is accomplished in conjunction with the franking systems and processes of the present invention), it is anticipated that the need for advanced filtering criteria and complex filter designs, features, and functions may be reduced. Additionally, processing of e-mails/communications 105 based upon whether such e-mails/communications are associated with a frank 110 may also minimize the likelihood that legitimate e-mails/communications are accidentally permanently discarded. Thus, one embodiment of the present invention may utilize frank 110 processing rules and systems in conjunction with e-mail/communication 105 filters 205 (and/or other known e-mail/communication processing devices) in order to determine when and whether to process and communicate e-mails/communications 105 to recipients.

Please replace the paragraph beginning at page 24, line 17, (paragraph [00067]) with the following paragraph, marked to show changes:

[00067] Another approach for reducing and/or eliminating undesired communications 105, such as spam, utilizes recipient permissions and approved sender lists. In general, a permission-based software application (not shown), such as CHOICE MAIL, may be loaded onto a recipient device 125 or utilized at an ISP 225 associated with a given recipient device 125. In this approach, the application generally does not try to identify and block spam (see, for example, the Wall Street Journal article "Choice Mail Designs Best Traffic Cop Yet to Thwart Spammers," July 11, 2002, incorporated herein by reference). Instead, the application determines whether a given sender has the recipient's permission to send the recipient an e-mail/communication 105. Upon belief, the CHOICEMAIL system and similar approaches may utilize a look-up table containing a list of approved senders. The look-up table may be stored on the recipient's device 125 or at a network node 135. Accordingly, whenever an e-mail/communication 105 from an unapproved sender is received, permission is requested or verified from the recipient prior to the e-mail/communication entering the recipient's e-mail/communication inbox.

Please replace the paragraph beginning at page 26, line 8, (paragraph [00070]) with the following paragraph, marked to show changes:

[00070] However, it is to be appreciated that certain embodiments of the present invention may utilize a franking system wherein unfranked e-mails/communications 105 are automatically discarded. In such an embodiment, it is foreseeable that an unfranked e-mail/communication 105 from a sender on a given recipient's approved sender list 235 might be discarded before reaching the recipient's ISP 225 and/or ~~presentation~~ device/system 125. As such, various embodiments of the present invention may also be configured such that approved sender lists 235 are communicated to clearing house servers (not shown). As used herein, "clearing house servers" generally remove an unfranked e-mail/communication 105 from a given network 120 unless the e-mail/communication is from an approved sender, as identified by a recipient's approved sender list 235. Currently, it is believed that most U.S. domestic Internet traffic passes through a handful of central servers. Such central servers may be configured to act as such clearing house servers. Similarly, large ISPs 215, 225 (such as AMERICA ONLINE, MSN, YAHOO, and others) might also be suitably configured as clearing house servers.

Please replace the paragraph beginning at page 27, line 1, (paragraph [00071]) with the following paragraph, marked to show changes:

[00071] Yet another embodiment may facilitate the communication of unfranked e-mails/communications 105 across a franked communications system or network 120. Accordingly, senders' systems 115 and/or associated servers ~~210~~ 215 may be configured to store approved sender list 235 information. Using this embodiment, the sender's system 115, ISP 215, or other network node 135 may attach a pseudo-frank of no or little value (instead of a fully valued frank) when sending e-mails/communications 105 to a recipient who has previously identified the sender as being on his approved sender list 235. In this manner, systems designed to automatically discard unfranked e-mails/communications 105 may function without concern for approved senders' e-mails/communications being mistakenly discarded, because of the pseudo-frank value associated with such e-mails/communications. It is to be appreciated that, upon identifying a sender on an approved sender list 235 or removing a sender from such list, the recipient's system 125, ISP 225, or other network node 135 may send an e-mail/communication 105 to the sender's system 115 or ISP 215 which deactivates pseudo-franking for the given recipient. Thus, various embodiments of the franking systems and processes of the present invention may be utilized in conjunction with approved sender lists 235 and the like.

Please replace the paragraph beginning at page 27, line 20, (paragraph [00073]) with the following paragraph, marked to show changes:

[00073] Fig. 3 shows an embodiment 300 of the present invention featuring a central franking server 305. Although only a single franking server 305 is shown in the embodiment of Fig. 3, in practice multiple franking servers may be employed. Each franking server 305 may, for example, be responsible for franking e-mails/communications ~~and/or other communications~~ provided by certain senders 115, network nodes 135, Internet service providers (ISPs) 215, 225 or their associated customers, geographical areas, network addresses, and so forth.

Please replace the paragraph beginning at page 28, line 4, (paragraph [00074]) with the following paragraph, marked to show changes:

[00074] The sender's ISP ~~210~~ 215 may include a sending e-mail server 320 and network connector 325. The network connector 325 may facilitate server 320 connection to the network 120.

Please replace the paragraph beginning at page 30, line 1, (paragraph [00078]) with the following paragraph, marked to show changes:

[00078] Upon receipt of the e-mail/communication 105, the franking server 305 determines the service class requested by the sender. The franking server 305 debits the sender's account 310 for the amount of the frank 110 (or simply confirms that the sender has pre-purchased a valid and legitimate frank of the appropriate class), attaches, associates or otherwise incorporates the frank 110 to the e-mail/communication 105, and transmits the now-franked e-mail/communication across the network 120 and to a recipient's e-mail/communication server ~~135~~ 315. The recipient's e-mail/communication server 135 may verify the authenticity of the frank 110 and, once the frank's authenticity is confirmed, transmit the franked e-mail/communication 105 to the recipient's system 125. Additionally, where bulk franking of e-mails/communications 105 occurs, the franking server 305 may be provided with a single copy of an e-mail/communication having multiple recipients, and may frank and deliver the bulk e-mail/communication appropriately. Finally, the e-mail/communication application 130 resident on the recipient's system 125 may classify the incoming e-mail/communication 105 according to its frank 110. The above activities may be performed either for a single e-mail/communication or a number of communications.

Please replace the paragraph beginning at page 32, line 22, (paragraph [00085]) with the following paragraph, marked to show changes:

[00085] Next, in operation 405, the purchased franks 110 are added to a sender's account. Generally speaking, the franking server may keep track of the number of franks currently associated with each sender. Such information could alternately be tracked by the sender's system ~~425~~ 115. That is, a certain number of franks 110, value of franks, number of franks in a given category, and so forth may be downloaded to and metered by the sender's system ~~425~~ 115, as described in more detail below.

Please replace the paragraph beginning at page 34, line 8, (paragraph [00088]) with the following paragraph, marked to show changes:

[00088] In operation 415, the desired frank 110 is "attached" to, otherwise associated with, or incorporated into the e-mail/communication 105. In the present embodiment, the frank 110 is attached to the ~~e-mail~~/communication 105 upon receipt of the e-mail/communication by the franking server 305. Thus, the franking server is responsible for assigning the appropriate service class to each e-mail/communication, as requested by the sender. In alternate embodiments, the franking server 305 may be split into multiple network entities, one of which keeps track of a sender's account 310 balance and is responsible for selling franks 110 to a sender, and another network entity which actually integrates the frank with the e-mail/communication 105. In yet another embodiment, the e-mail/communication may be franked by the sender's system ~~425~~ 115, the sender's e-mail/communication server ~~315~~ 320, the sender's ISP 215, or another network node 135 associated with the sender. In any regard, once the e-mail/communication 105 has been franked, it is routed to the franking server 305 for transmission to the recipient's ISP 225 or e-mail/communication server 315 in operation 420. Finally, in step ~~430~~ 440, the ~~e-mail~~/communication is delivered.

Please replace the paragraph beginning at page 37, line 19, (paragraph [00096]) with the following paragraph, marked to show changes:

[00096] An alternate embodiment may add to the approved sender list 235 all senders to whom the recipient has replied or otherwise initiated a e-mail/communication 105 within a certain time period, such as six months or one year. Time periods may be set by the embodiment or the user. In the event the recipient does not transmit [[a]] an e-mail/communication 105 to a sender within a time period, the sender may be removed from the recipient's approved list 235. Similarly, an alternate embodiment may add to an approved sender list those senders whose e-mails/communications have been accessed by a recipient within a certain time frame. Again, should the recipient not open or otherwise access the sender's e-mail/communication 105 after a certain time expires, that specific

sender may be manually or automatically removed from the recipient's approved sender list 235.

Please replace the paragraph beginning at page 46, line 5, (paragraph [000117]) with the following paragraph, marked to show changes:

[000117] Fig. 8 displays a portion of an embodiment 800 detailing the purchase of one or more franks 110. In the embodiment 800 shown in Fig. 8, the franking application 805 may interact with either a browser 705, an e-mail/communication application program 605, or directly with an output device manager 610, as represented by the dashed arrows. In alternate embodiments, the franking application 805 may interact with only one or two of the three other elements 605, 610, 705, or may be integrated as a sub-program in one or more of these elements. Further, although a database 615 is shown as a separate program or piece of code, it too may be directly integrated with the franking application 600, 700, 805, e-mail/communication application program 605, browser 705, or output device manager 610.

Please replace the paragraph beginning at page 46, line 16, (paragraph [000118]) with the following paragraph, marked to show changes:

[000118] Generally, a sender may initiate a frank ~~115~~ 110 purchase through one of the variety of methods mentioned in the section above. As part of this initiation, the sender may specify one or more criteria for the frank 110. For example, the sender may specify a class of frank, frank value, number of franks desired, frank expiration date, frank encryption method, frank usage time (that is, time periods at which a frank may be valid- for example, from 6am to 6pm, or from 10pm to 4 am, or any other start and end time), and so on. It should be noted that a frank usage time is different from a frank expiration date- the first specifies a period of time during a day, week, month, and so forth during which a frank may be attached to an e-mail/communication and accepted by a franking server, while the second specifies a time after which the frank will no longer be valid. Further, the frank expiration date may be specified as the end of a time period, or a certain date. For example, a frank 110 with a 1:00 p.m. – 6:30 p.m. frank usage time and a three month frank expiration date may be used to frank an e-mail/communication 105 transmitted between 1:00 and 6:30 p.m. on any day during the three months after the purchase date. Additionally, the sender may specify a payment method, as discussed above.

Please replace the paragraph beginning at page 48, line 21, (paragraph [000123]) with the following paragraph, marked to show changes:

[000123] Alternately, the previously-mentioned card may contain data identifying a default set of franks 110, for example specifying a number of desired franks and classes or attributes for each. When the card is inserted into or swiped through the kiosk, the kiosk may automatically place the number and type of franks 110 specified by the data onto the card, and debit an account ~~305~~ 310 associated with the purchaser. Yet alternately, the default frank set may be presented as a purchase option, rather than being automatically filled.

Please replace the paragraph beginning at page 53, line 18, (paragraph [000139]) with the following paragraph, marked to show changes:

[000139] Alternately, franked e-mails/communications 105 may be authenticated by passing such franked e-mails/communications through a gatekeeper. One example of a gatekeeper system configuration is shown in Fig. 9A, where the central franking server 905 may act as a gatekeeper. In this configuration, Internet service providers 215/225 and/or independent franking nodes 135 may be utilized to approve and/or attach a frank 110 to an e-mail/communication 105. Requests for franks may be routed to one of these approved network entities 900, 905, 910. The network entities, in turn, would generate the frank 110 and attach it to the e-mails/communications 105.

Please replace the paragraph beginning at page 54, line 16, (paragraph [000143]) with the following paragraph, marked to show changes:

[000143] In addition to the franks 110 and various implementations of an address list ~~235disclosed~~ 235 disclosed herein, an embodiment of the present invention may be configured to operate with a code, a password, or other identifier embedded or otherwise attached to the e-mail/communication 105. For example, one embodiment may be configured to automatically frank any outgoing e-mails/communications 105 including such a code, or to treat any incoming e-mails/communications containing such a code as a franked e-mail/communication. Effectively, the code may act as a frank 110 of any sort described (or any combination of franks described) herein, without requiring payment from the sender.

Please replace the paragraph beginning at page 55, line 3, (paragraph [000144]) with the following paragraph, marked to show changes:

[000144] For example, a recipient may provide a code to a sender. Rather than franking an email/communication 105, as described herein, the sender may include the code in the body of the email/communication, its subject line, another portion of the email/communication, or otherwise attach or associate the code with the

email/communication. Upon receipt of the email/communication 105 contained in the code, the recipient's ISP 225, or mail server 315, or mail application program 130 may verify the code. If the code is properly authenticated (for example, by comparing it against a list of recipient-specified codes or matching the code to a recipient's key), the recipient's ISP, mail server, or mail application program may deliver or otherwise queue the email/communication 105 as if the e-mail/communication were franked with a frank 110 of the type corresponding to the code. Alternately, the recipient's ISP 225, mail server 315, or mail application program 130 may generate a pseudo-frank of the type associated with the code and attach the pseudo-frank to the communication 105. By generating and attaching the pseudo-frank, the embodiment may facilitate processing the e-mail/communication 105 (including the code) according to the standard franking rules of the recipient's mail server 315, mail application program ~~130, or~~ 130, or franking application 805, without requiring exceptions to those rules for e-mails/communications 105 having codes. Further, in an embodiment displaying the frank 110 type or class associated with the e-mail/communication 105 in a recipient's mailbox or folder structure, generating and attaching a pseudo-frank insures the embodiment displays the coded e-mail/communication in the same manner as any franked e-mail/communication received. Thus, visual continuity regarding the display of emails/communications 105 may be preserved by the embodiment.

Please replace the paragraph beginning at page 57, line 7, (paragraph [000147]) with the following paragraph, marked to show changes:

[000147] The embodiment may be configured to permit such codes to change in response to various criteria, thus eliminating the service life of a code and minimizing the likelihood of inappropriate use. For example, an embodiment may recognize a specific code only once, ignoring the presence of the code in any e-mails/communications 105 after the first. Alternately, the code may be valid for a set period of time, a random period of time, a user's specified time period, and so on. The code could be encrypted either electronically or biometrically, as may the e-mail/communication to which the code is attached. Further, the code may specify to the recipient's ISP 225 (or other nodes 210, ~~225, 135~~ 215, 315 in the e-mail/communication 105 transmission path) that the e-mail/communication 105 should be transmitted from the sender to the recipient, rather than being purged or deleted. Codes may be unique to individuals, or may be shared by companies, organizations, ISPs, Internet domains, and so on.

Please replace the paragraph beginning at page 59, line 12, (paragraph [000155]) with the following paragraph, marked to show changes:

[000155] In addition to the sorting, filtering, and valuation concepts discussed above, at least one embodiment of a franking system may be configured to provide additional unique enhancements to the transmission and receipt of e-mails/communications 105. For example, an electronic equivalent of certified postal mail may be implemented through an embodiment of the present invention. By requesting certified delivery of franked e-mails/communications 105, a sender may receive confirmation of the delivery of the e-mail/communication to the recipient. Generally, this confirmation is generated by either a franking application 805, 130 resident on the receiving e-mail/communication server 315, the receiving e-mail/communication application 130, a receiving system 125, or other network node 135 responsible for transmitting the franked e-mail/communication to the receiving e-mail/communication server. Some time after receipt of a certified franked e-mail/communication 105, one of the above may create a confirmation e-mail/communication indicating that the certified franked e-mail/communication has been received by the node 135. Optionally, the confirmation e-mail/communication 105 may include additional data, such as the time of receipt, whether or not the recipient has reviewed the certified franked e-mail/communication, an identifier corresponding to either the frank 110 or the certified franked e-mail/communication 105 itself, an identifier indicating the network or system element 135 generating the confirmation e-mail/communication, and so forth. Once created, the confirmation e-mail/communication may be transmitted across the network ~~120to~~ 120 to the sender's system.

Please replace the paragraph beginning at page 61, line 14, (paragraph [000159]) with the following paragraph, marked to show changes:

[000159] In addition to the delivery receipt function described above, the certified mail features of the franking systems described herein may include a tracing function. That is, when a franked e-mail/communication 105 is certified for delivery, its path through the network 120 from the sending e-mail/communication server ~~210to~~ 210 to the receiving e-mail/communication server 225 may be logged. Typically, this log takes the form of a series of network addresses. The log may also indicate whether an e-mail/communication 105 was copied or stored at a network node. Optionally, the copying and storage elements of the log may be available only if an additional frank 110 is purchased.

Please replace the paragraph beginning at page 69, line 3, (paragraph [000182]) with the following paragraph, marked to show changes:

[000182] Generally, it should be noted that an e-mail/communication 105 from an approved sender, domain, or even franked e-mails/communications received from a verified franking server 305, 900, 905, 910 may also be filtered or processed according to the standard rules of the receiving e-mail/communication server ~~215~~ 315, the recipient system 125, or the recipient's e-mail/communication application program 130. That is, simply franking an e-mail/communication 105 or adding a domain or sender to an approved list 235 may not circumvent virus checking software and so forth.

Please replace the paragraph beginning at page 79, line 4, (paragraph [000208]) with the following paragraph, marked to show changes:

[000208] Essentially, when an authorized sender initiates an e-mail/communication 105 across the ~~franking system~~ network 120, 915, and classified as one of these ultra-high categories, the e-mail/communication is specially franked and transmitted as above. However, instead of transmitting the franked e-mail/communication 105 to a single recipient or list of recipients, all (or a sub-set of) network nodes 135 and ISPs 215, 225 associated or in communication with the ~~franking system~~ network 120, 915 may be configured to receive the franked e-mail/communication 105. Further, such nodes 135 may receive instructions to disseminate the franked e-mail/communication 105 to all registered system recipients.

Please replace the paragraph beginning at page 80, line 12, (paragraph [000212]) with the following paragraph, marked to show changes:

[000212] [[A]] With reference now to Fig. 10, a telemarketer or other caller may contact a franking server 1000 to purchase one or more franks 110 via his telephone ~~1030,~~ 1030, as detailed with respect to Figs. 6-8. The franking server 1000 may, for example, include a franking interface 1005 for handling a frank request initiated from a caller's system 1010, as well as distributing purchased franks. The franking server 1000 may also include an account list 1015 maintaining a list of all senders who have established an account 310 with the franking server. For reference, previously-discussed franking servers 305, 900, 905, 910 may also include these elements 1000, 1005.

Please replace the paragraph beginning at page 81, line 7, (paragraph [000214]) with the following paragraph, marked to show changes:

[000214] Once the franked call 105 is received by a network node 1020, the telephone network node may verify the frank's 110 authenticity. Generally, this verification may take place using any of the methods previously described. The telephone network

node 1020 may then connect the call to the recipient's telephone 1025. The frank class and related information may be displayed on the recipient's caller identification equipment, telephone, or any other device connected to the telephone network ~~1040~~ 1045 and capable of displaying alphanumeric information or providing unique ring patterns.